IP EYE ANYWHERE™

IP EYE ANYWHERE 241/341

Advanced Installation Guide

20377 / 20110202 • IP EYE ANYWHERE 241/341™
ALL RIGHTS RESERVED MARMITEK ©

MARMITEK®

Preface

Thank you for purchasing the Marmitek H.264/MPEG4/MJPEG Day&Night or True Colour Megapixel Network Camera, a standalone system that can be connected directly to an Ethernet or Fast Ethernet network.

Equipped with a megapixel CMOS sensor, the camera allows you to capture a wider field of view with a resolution of up to 1280 x 1024. With support for latest H.264 technology, you can record streaming video that utilizes high quality H.264 images to your hard drive, enable motion detection and setup automated e-mail alerts for security.

With the Infrared LEDs and light sensor on the camera (IPEA 241 only), you can capture clear images even in the dark environment.

Compared to the conventional PC Camera, this camera features a built-in CPU and web-based solutions that can provide a cost-effective solution to transmit the real-time high-quality video images and sounds synchronously for monitoring. The camera can be managed remotely, so that you can use a web browser to access and control it from any desktop/notebook computer over the Intranet or Internet.

The simple installation procedures and web-based interface allow you to integrate it into your network easily. With comprehensive applications supported, the IPEyeAnywhere 241 / 341 is your best solution for remote monitor, high quality, and high performance video images.

This *Advanced Installation Guide* provides you with the instructions and illustrations on how to use your camera, which includes:

Chapter 1 **Introduction to Your Camera** describes the features of the camera. You will also know the components and functions of the camera.

Chapter 2 **Hardware Installation** helps you install the camera according to your application environment. You can use this camera at home, at work, at any where you want.

Chapter 3 **Accessing the Camera** lets you start using your camera without problem. The camera can be set up easily and work within your network environment instantly.

Chapter 4 **Configuring the Camera** guides you through the configuration of the camera using the Web browser on your PC.

Chapter 5 **Appendix** provides the specification of the camera and some useful information for using your camera.

NOTE The illustrations and configuration values in this guide are for reference only. The actual settings depend on your practical application of the camera.

Contents

CHAPTER 1 5
INTRODUCTION TO YOUR CAMERA 5
1.1 CHECKING THE PACKAGE CONTENTS 5
1.2 GETTING TO KNOW YOUR CAMERA 6
1.3 FEATURES AND BENEFITS 10
1.4 SYSTEM REQUIREMENT 13
CHAPTER 2 14
HARDWARE INSTALLATION 14
2.1 INSTALLING THE CAMERA STAND 14
2.2 CONNECTING THE CAMERA TO LAN/WLAN 15
2.3 APPLICATIONS OF THE CAMERA 16
CHAPTER 3 17
ACCESSING THE CAMERA 17
3.1 USING IPFINDER 17
3.2 ACCESSING TO THE CAMERA 18
3.3 CONFIGURING THE IP ADDRESS OF THE PC 21
CHAPTER 4 22
CONFIGURING THE CAMERA 22
4.1 USING THE WEB CONFIGURATION 22
4.2 QUICK SETUP 23
4.3 BASIC SETUP 30
4.4 NETWORK SETTINGS 33
4.5 SETTING UP VIDEO & AUDIO 41
4.6 EVENT SERVER CONFIGURATION 46
4.7 MOTION DETECT 52
4.8 EVENT CONFIGURATION 53
4.9 TOOLS 56
4.10 USB 58
4.11 INFORMATION 60
Appendix 61
A.1 SPECIFICATION 61

SAFETY WARNINGS

• To prevent short circuits, this product should only be used inside and only in dry spaces.

• Do not expose the components to rain or moisture. Do not use the product close to a bath, swimming pool etc.

• Do not expose the components of your systems to extremely high temperatures or bright light sources.

• In case of improper usage or if you have altered and repaired the product yourself, all guarantees expire. Marmitek does not accept responsibility in the case of improper usage of the product or when the product is used for purposes other than specified. Marmitek does not accept responsibility for additional damage other than covered by the legal product responsibility.

• This product is not a toy. Keep out of reach of children.

• Do not open the product: the device may contain live parts. The product should only be repaired or serviced by a qualified expert.

• Only connect the adapter to the mains after checking whether the mains voltage is the same as the values on the identification tags. Never connect an adapter when it is damaged. In that case, contact your supplier.

CHAPTER 1

INTRODUCTION TO YOUR CAMERA

1.1 Checking the Package Contents

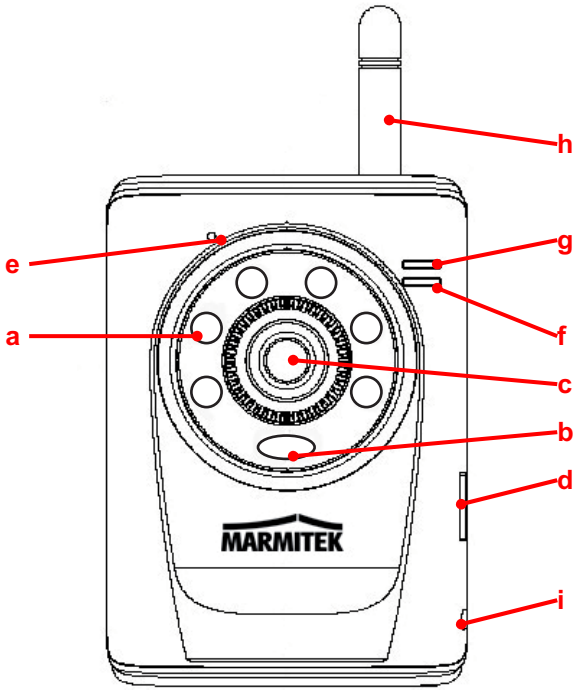
Check the items contained in the package carefully. You should have the following:

- ☑ One IPEyeAnywhere 241 / 341 Network Camera
- ☑ One AC Power Adapter
- ☑ One Camera Stand
- ☑ One External Antenna
- ☑ One Ethernet Cable (RJ-45 type)
- ☑ One Installation CD-ROM
- ☑ One *Quick Installation Guide*

NOTE Once any item contained is damaged or missing, contact the authorized dealer of your locale.

1.2 Getting to Know Your Camera

■ Front / Right Panel



a. Infrared LEDs (x6) allow your camera to capture clear image in a dark environment (IPEA 241 only).

b. Light Sensor is used to trigger on and off the Infrared LEDs according the environmental light level.(IPEA 241 only)

c. Lens Assembly

d. **USB Port** allows you to connect an external USB device. It provides the power distribution up to 500mA.

e. **Internal Microphone** allows the camera to receive sound and voice.

f. **Link LED** indicates the camera's network connectivity with the flashing green light.

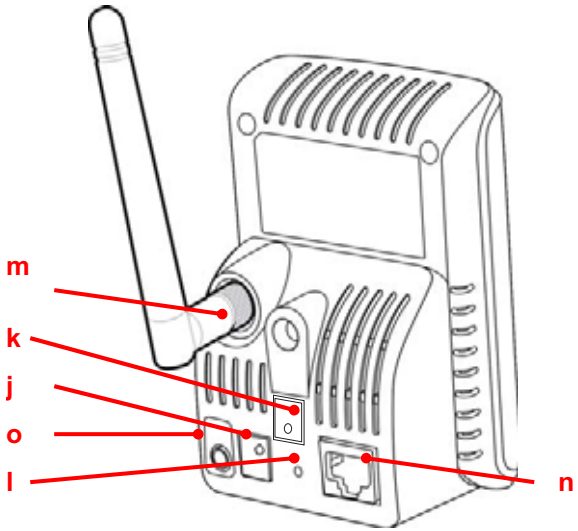
g. **Power LED** indicates the camera is powered on with the steady amber light.

h. **External Antenna**

i. **USB* Unmount Button** Is used to remove the connected USB device safely.

NOTE After long pressing the Unmount button for four seconds, the Power LED starts flashing. When the Power LED resumes the steady amber light, you can remove the USB device safely.

■ Rear Panel



j. DC Power Connector connects the AC power adapter, in order to supply power to the camera.

k. WPS Button is used to protect your WLAN. Instead of entering the network name (SSID), your wireless network can be protected simply by pushing a button.

TIP For more information of using the WPS button, refer to the instruction of the Web Configuration, Network >> Wireless >> WPS Setting.

l. Reset Button will restart the camera when it is pressed quickly; when it is pressed and held for five seconds, the camera will resume the factory default settings.

m. Wireless Antenna Connector is used to attach the external antenna.

n. **Ethernet Cable Connector** connects the network cable, which supports the NWay protocol so that the camera can detect the network speed automatically.

o. **Audio-out Connector** connects an external active speaker.

1.3 Features and Benefits

- **H.264/MPEG4/MJPEG Multi-codec Supported**

  The IPEyeAnywhere 241 / 341provides you with excellent images by the H.264/MPEG4/ MJPEG multi-codec selectable technology, allowing you to adjust image size and quality, and bit rate according to the networking environment.

- **High Resolution Surveillance**

  Equipped with a megapixel CMOS sensor, the high performance camera is designed for your professional surveillance and security applications. The image resolution is up to 1280 x 1024.

- **IPEA241: Day & Night Surveillance Supported**

  The six Infrared LEDs around the standard lens assembly enable the camera to capture crystal clear images in the dark environment or at night. When the Light Sensor detects the environmental light level becomes low, the camera captures the images in black & white mode using these infrared LEDs.

- **IPEA341: True Colour Camera**

  The camera has a IR blocking filter to produce accurate colours. It blocks the transmission of the infrared while passing the visible.

- **Remote Control Supported**

  By using a standard Web browser or the bundled UltraView Pro software application, the administrator can easily change the configuration of the camera via Intranet or Internet. In addition, the camera can be upgraded remotely when a new firmware is available. The users are also allowed to monitor the image and take snapshots via the network.

- **Multiple Profiles Supported**

  The camera supports multiple profiles simultaneously, so that you can separately set up different image settings (such as image quality and frame rate) for the video types of the camera: H.264, MPEG4, MJPEG, and 3GPP.

- **Flexible Audio Capability**

  The built-in microphone of the Marmitek IP EyeAnywhere 241 / 341 camera provides on-the-spot audio via the Internet, allowing you to monitor the on-site voice. In addition, you can connect an external speaker to the camera to speak through the camera. (supporting mono audio only).

- **Supports RTSP**

  The camera supports RTSP (Real Time Streaming Protocol), which is a technology that allows you to view streaming media via the network. You can view the real-time video with the Quick Time player or RealPlayer. To view the real-time streaming image on your computer, open the Web browser and enter the RTSP link:

  MPEG4 stream: rtsp://(IP address of the camera)/mpeg4

  H.264 stream: rtsp://(IP address of the camera)/h264

- **Mobile Device Viewing Supported**

  The camera supports real time video viewing on your mobile device. After installing the required software applications, you can easily monitor the camera's real-time video from your iPhone, iPod Touch, or iPad (requires iPhone OS 3.1 or later). The latest Android phone can be supported too.

- **Multiple Platforms Supported**

  The camera supports multiple network protocols, including TCP/IP, SMTP e-mail, HTTP, and other Internet related protocols. Therefore, you can use the camera in a mixed operating system environment, such as Windows 2000/XP/ Vista, and Windows 7/8.

- **Multiple Applications Supported**

  Through the remote access technology, you can use the cameras to monitor various objects and places for your own purposes. For example, babies at home, patients in the hospital, offices and banks, and more. The camera can capture both still images and video clips, so that you can keep the archives and restore them at any time.

1.4 System Requirement

- **Networking**
  - **LAN:** 10Base-T Ethernet or 100Base-TX Fast Ethernet; Auto-MDIX.
  - **WLAN:** IEEE 802.11b/g/n
- **Accessing the Camera using Web Browser**
  - **Platform:** Microsoft® Windows® XP/Vista/WIN 7/8
  - **CPU:** Intel Pentium III 800MHz or above
  - **RAM:** 512MB
  - **Resolution:** 800 x 600 or above
  - **User Interface:** Microsoft® Internet Explorer 6.0 or above; Apple Safari 2 or above; Mozilla Firefox 2.00 or above
- **Accessing the Camera using UltraView Pro**
  - **Platform:** Microsoft® Windows® XP/Vista/WIN 7/8
  - **Resolution:** 1024 x 768 or above
- **Hardware Requirement:**
  - **1 camera:** Intel Pentium 4 2.4GHz; 512MB RAM
  - **2~4 cameras:** Intel Pentium 4 2.8GHz; 1GB RAM
  - **5~16 cameras:** Intel Pentium 4 3.4Hz; 2GB RAM
  - **17~24 cameras:** Intel Core 2 Duo E6400; 1GB RAM
  - **25~32 cameras:** Intel Core 2 Duo E8400; 2GB RAM

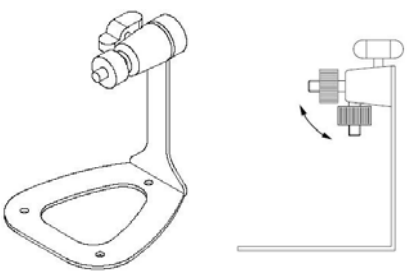
NOTE If you connect multiple cameras to monitor various places simultaneously, you are recommended to use a computer with higher performance.

CHAPTER 2

HARDWARE INSTALLATION

2.1 Installing the Camera Stand

The Marmitek IP Eye Anywhere camera comes with a camera stand, which uses a swivel ball screw head to lock to the camera's screw hole. When the camera stand is attached, you can place the camera anywhere by mounting the camera through the three screw holes located in the base of the camera stand.



2.2 Connecting the Camera to LAN/WLAN

Use the provided Ethernet cable to connect the Marmitek IP Eye Anywhere camera to your local area network (LAN).

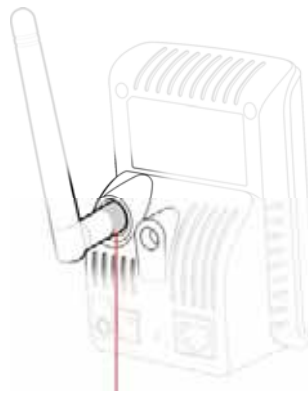
When you connect the AC power adapter, the camera is powered on automatically. You can verify the power status from the Power LED on the front panel of the camera.

Once connected, the Link LED starts flashing green light and the camera is on standby and ready for use now.

Connecting the Ethernet Cable

If you have the IEA11 or 21 and use a wireless network in your application environment, you need to attach the included external antenna to the camera.

When the camera is powered on, the camera will automatically search any access point with “default” SSID.



Connecting the External Antenna

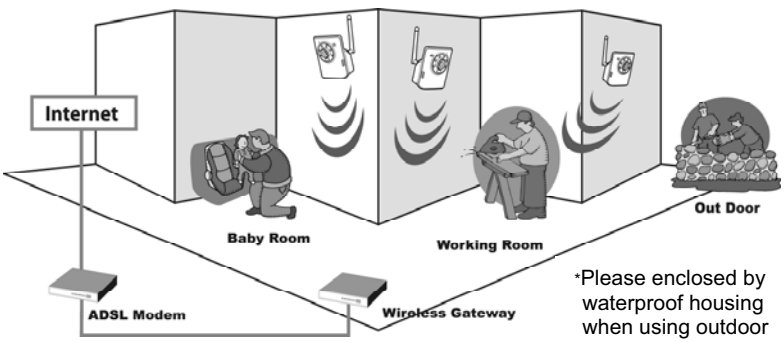
NOTE If the camera cannot connect to your wireless network, you need to install the camera in LAN and proceed with WLAN settings.

2.3 Applications of the Camera

The camera can be applied in multiple applications, including:

- Monitor local and remote places and objects via Internet or Intranet.
- Capture still images and video clips remotely.
- Upload images or send email messages with the still images attached.

The following diagram explains one of the typical applications for your camera and provides a basic example for installing the camera.



Home Applications of the Internet Cameras

***** Please have the camera enclosed by waterproof housing when using in outdoor.

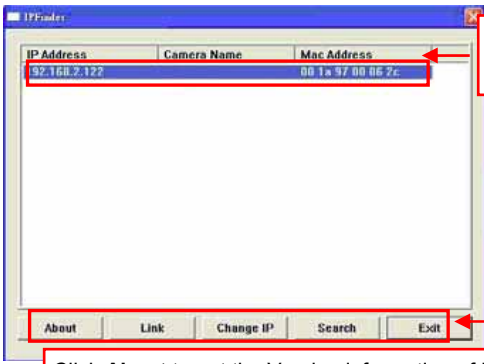
CHAPTER 3

ACCESSING THE CAMERA

3.1 Using IPFinder

The camera comes with a conveniently utility, IPFinder, which is included in the Installation CD-ROM, allowing you to search the camera on your network easily.

1. Insert the Installation CD-ROM into your computer's CD-ROM drive to initiate the Auto-Run program.
2. Click the **IPFinder** item to launch the utility. The control panel will appear as below.

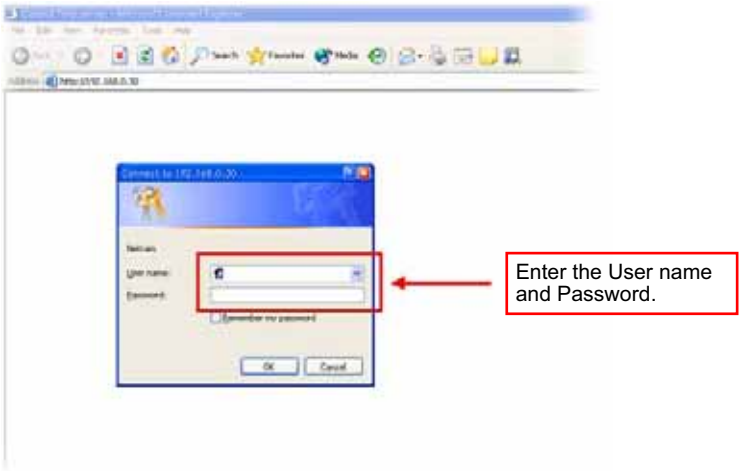

IPFinder
IP Address
Camera Name
Mac Address
192.168.2.122
00 1a 97 00 06 7c
About
Link
Change IP
Search
Exit
Display the connected camera(s). Double click to link the Camera.
Click About to get the Version information of IPFinder.
Click Link to connect the selected camera.
Click Change IP to modify the IP address of the selected camera.
Click Search to find the IP address of the connected camera(s).
Click Exit to close the utility.

3. Once you get the IP address of the camera, launch the Web browser or UltraView Pro to access your camera.

3.2 Accessing to the Camera

Whenever you want to access the camera:

1. Since the default configuration of the camera is DHCP mode enabled, you are recommended to launch IPFinder to search the IP address that is assigned to the camera by the DHCP server, and then click **Link** to access the camera via the Web browser.
2. If Network Camera can't get IP Address under DHCP mode, the default IP Address will be 192.168.0.30.
3. When the login window appears, enter the default User name (admin) and password (admin) and press **OK** to access to the main screen of the camera's Web Configuration.



NOTE If you are initially access to the camera, you will be ask to install a new plug-in for the camera. Permission request depends on the Internet security settings of your computer. Click Yes to proceed.

After you login into the Web Configuration of the camera, the Main screen will appear as below:

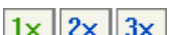
The Main screen of the Web Configuration provides you with many useful information and functions, including:

1. **Live View/Setup Switch:**
   - Click the SET-UP button to configure the camera. For details, see Chapter 4.
   - Click the LIVE VIEW button to return to the Main screen to view the live view image.
2. **Compression Buttons:** Select to transmit and record the video using **H.264**, **MPEG4** or **MJPEG** compression.

❸ **Function Buttons:** Use these buttons to control the audio, video, and trigger functions.

- **Manual Record** allows you to record and save a video clip.
- **Snapshot** allows you to capture and save a still image.
- **Browse** allows you to assign the destination folder to store the video clips and still images.
- **Talk** allows you to speak out through the camera. Please note only one user is allowed to use this function at a time.
- **Listen** allows you to receive the on-site sound and voice from the camera.

❹ **Live View Area:** Displays the real-time video image of the connected camera.

- The **Compression mode** is displayed above the Live View image.
- Click the **Zoom buttons** () to zoom in the live view image by **1x**, **2x**, or **3x**.

❺ **Language and Camera Information:**

- The **Language** pull-down menu allows you to select your favorite displayed language for the system.
- The **Camera Information** area displays the camera's location and the current date & time. The information can be modified in the Web Configuration.

NOTE If your PC use Microsoft Vista platform, you may not find the recorded files that are saved by **Snapshot** or **Manual Record**. You need to disable the protected mode of Security in the IE Browser through the following steps:

1. Open the Internet Explorer browser.
2. Click **Tools > Internet Options**.
3. Click **Security**.
4. Disable the **Enable Protected Mode** option and then click **OK**.

3.3 Configuring the IP Address of the PC

If you are failed to access to the camera, please check the IP address of your computer. When you connect the camera to your computer directly to proceed with configuration of the camera, you need to set up the IP addresses to be in the same segment for the two devices to communicate.

1. On your computer, click **Start > Control Panel** to open the Control Panel window.
2. Double-click **Network Connection** to open the Network Connection window.
3. Right-click **Local Area Connection** and then click **Properties** from the shortcut menu.
4. When the Local Area Connection Properties window appears, select the **General** tab.
5. Select **Internet Protocol [TCP/IP]** and then click **Properties** to bring up the Internet Protocol [TCP/IP] Properties window.
6. To configure a fixed IP address that is within the segment of the camera, select the **Use the following IP address** option. Then, enter an IP address into the empty field. The suggested IP address is 192.168.0.x (x is 1~254 except 30), and the suggested Subnet mask is 255.255.255.0.
7. When you are finished, click **OK**.

CHAPTER 4

CONFIGURING THE CAMERA

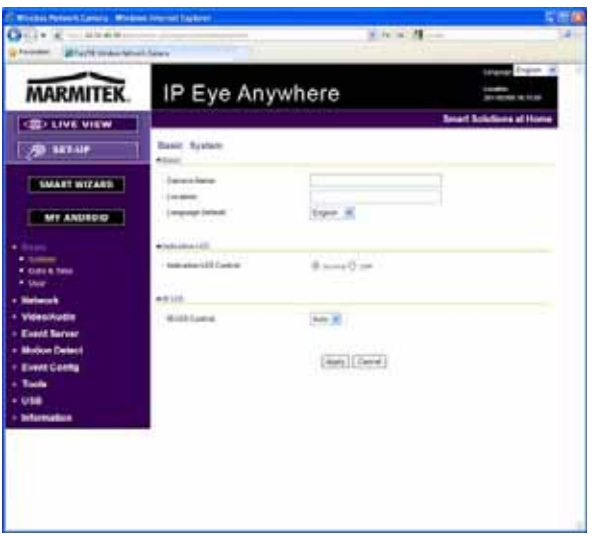
4.1 Using the Web Configuration

You can access and manage the camera through the Web browser and the provided software application UltraView Pro. This chapter describes the Web Configuration, and guides you through the configuration of the camera by using the Web browser.

To configure the camera, click

on the Main screen of Web Configuration. The Web Configuration will start from the **Basic** page.

The Web Configuration contains the settings that are required for the camera in the left menu bar, including **Smart Wizard**, **My Android**, **Basic**, **Network**, **Video/Audio**, **Event Server**, **Motion detect**, **Event Config**, **Tools**, **USB**, and **Information**.



© MARMITEK

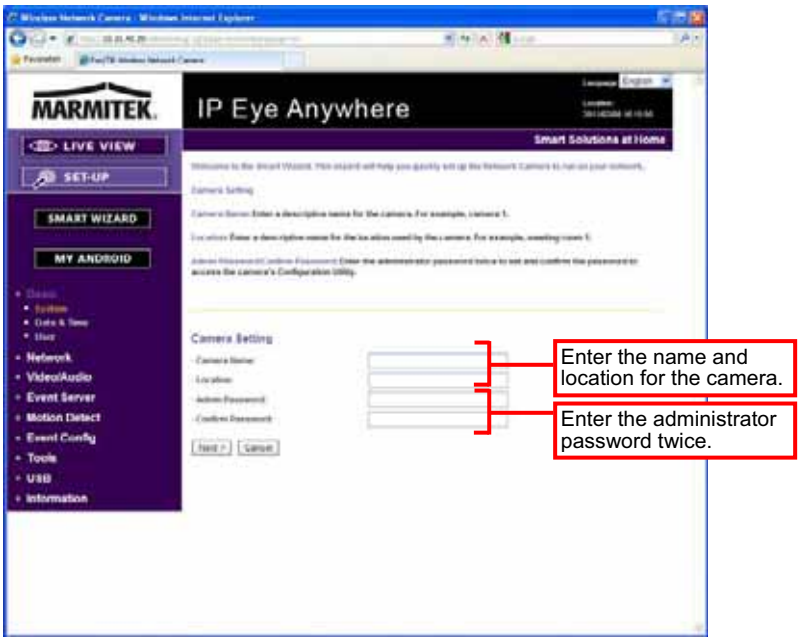
4.2 Quick Setup

4.2.1 Using Smart Wizard

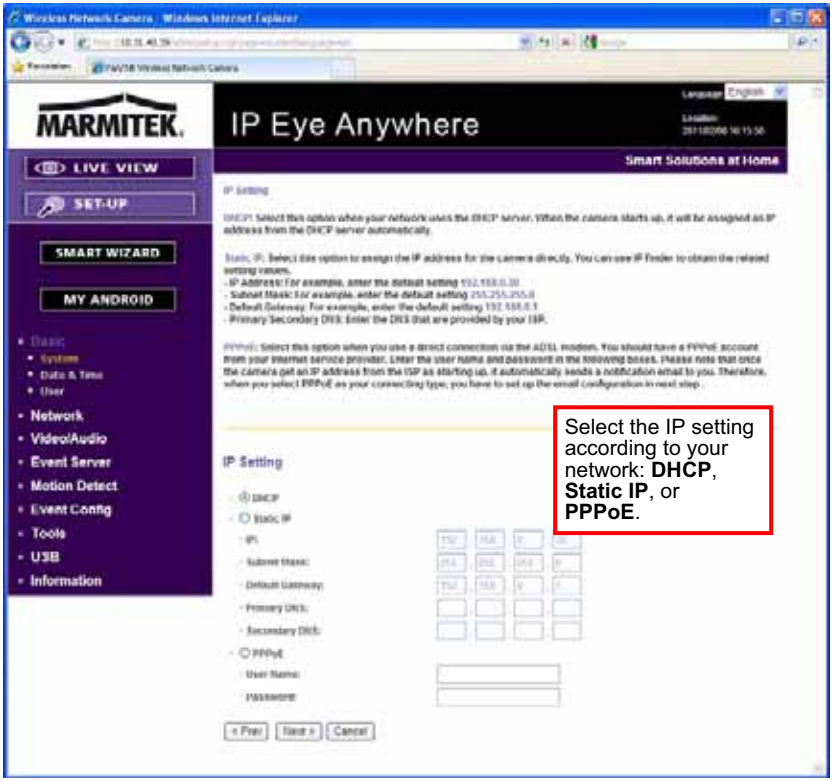
The camera's Smart Wizard lets you configure your camera easily and quickly. The wizard will guide you through the necessary settings with detailed instructions on each step.

To start the wizard, click **Smart Wizard** in the left menu bar.

Step 1. Camera Settings

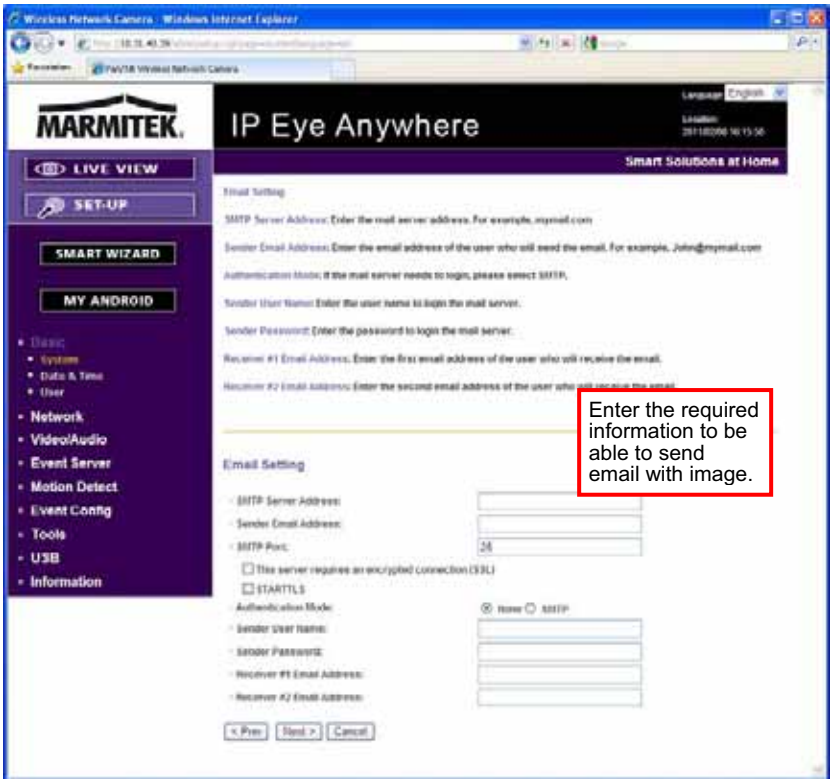


Step 2. IP Settings

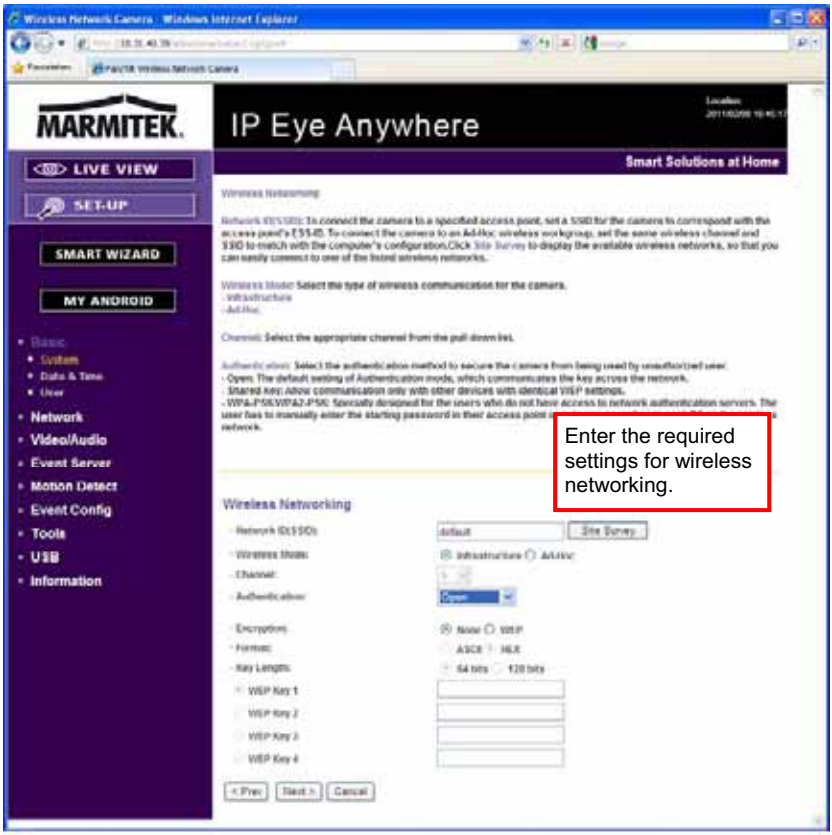


 © MARMITEK

Step 3. Email Settings

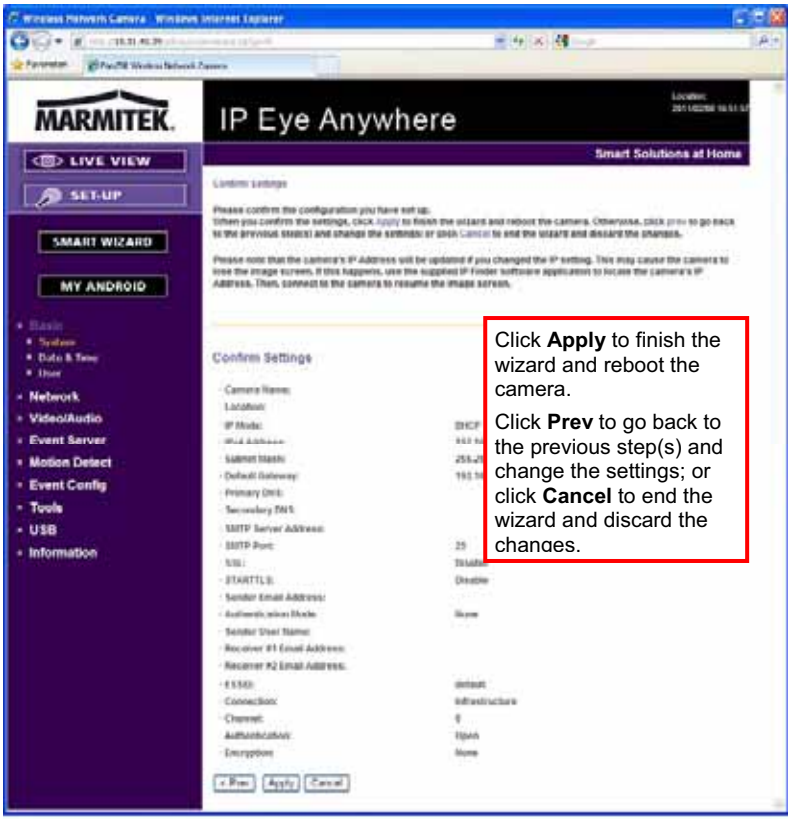


Step 4. Wireless Networking



© MARMITEK

Step 5. Confirm Settings



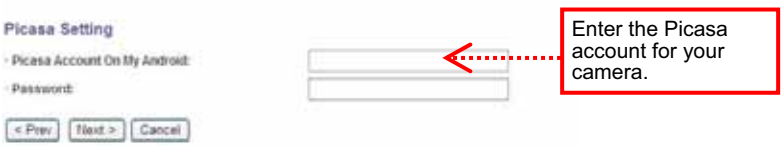
4.2.2 Using My Android

The camera's My Android wizard lets you set up your Android mobile and Google services (Google Talk and Picasa) easily and quickly. The wizard will guide you through the necessary settings with detailed instructions on each step.
To start the wizard, click **My Android** in the left menu bar.

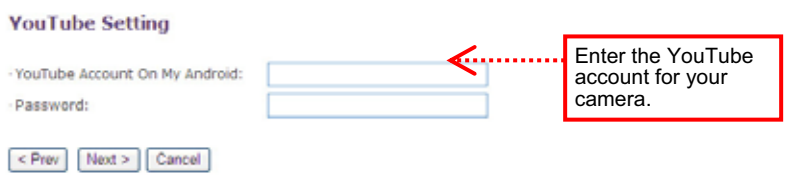
Step 1. Setting Up Google Talk Account

Step 2. Setting Up Gmail Account

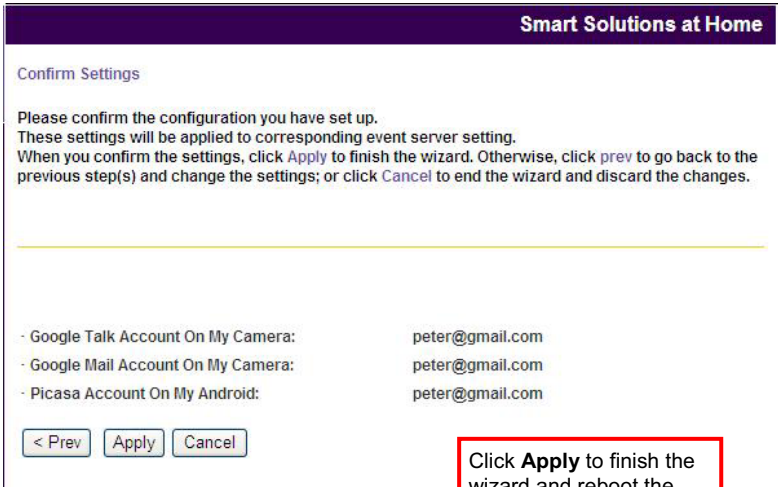
Step 3. Setting Up Picasa Account



Step 4. YouTube Settings



Step 5. Confirm Settings


Smart Solutions at Home
Confirm Settings
Please confirm the configuration you have set up.
These settings will be applied to corresponding event server setting.
When you confirm the settings, click Apply to finish the wizard. Otherwise, click prev to go back to the previous step(s) and change the settings; or click Cancel to end the wizard and discard the changes.
· Google Talk Account On My Camera: peter@gmail.com
· Google Mail Account On My Camera: peter@gmail.com
· Picasa Account On My Android: peter@gmail.com
< Prev
Apply
Cancel

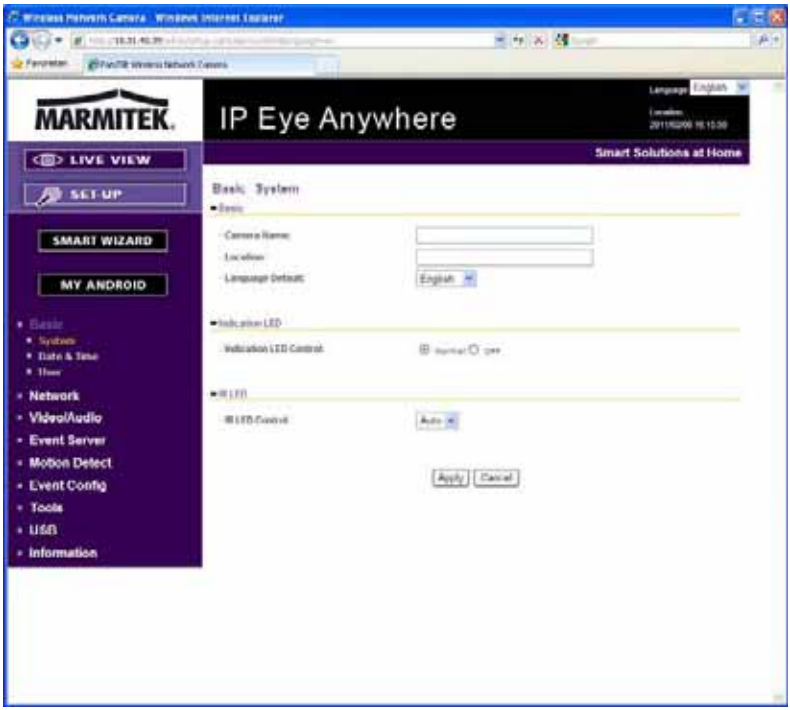
Click **Apply** to finish the wizard and reboot the camera.

Click **Prev** to go back to the previous step(s) and change the settings; or click **Cancel** to end the wizard and discard the changes.

NOTE Once you have set your Gmail account in step 2, the Email setting in Event Server Setting will be completed automatically. For more information, refer to the instruction of the Web Configuration, Event Server Setting >> Email.

4.3 Basic Setup

The Basic menu contains three sub-menus that provide the system settings for the camera, such as the Camera Name, Location, Date & Time, and User management.



4.3.1 Basic >> System

- **Basic:** This item allows you to assign the camera name and location information.
  - **Camera Name:** Enter a descriptive name for the camera, which is helpful to identify the camera easily while multiple cameras are connected within the network.

- **Location:** Enter a descriptive name for the location where is monitored by the camera.
- **Language Default:** Select your favorite displayed language for the system.

- **Indication LED Control:** This item allows you to set the LED illumination as desired. The available options include: **Normal** and **OFF**.
- **IR LED Control:** This item allows you to control the IR LED. The available options include: **Auto** and **OFF**.
  When **OFF** is selected you can select the start and end time when the IR LEDS have to be off. (IPEA 241 only)

4.3.2 Basic >> Date & Time

- **Date and Time:** Enter the correct date and time for the system.
  - **TimeZone:** Select the proper time zone for the region from the pull-down menu.
  - **Synchronize with PC:** Select this option and the date & time settings of the camera will be synchronized with the connected computer.
  - **Synchronize with NTP Server:** Select this option and the time will be synchronized with the NTP Server. You need to enter the IP address of the server and select the update interval in the following two boxes. (For example 131.155.2.3)
  - **Manual:** Select this option to set the date and time manually.

4.3.3 Basic >> User

- **Administrator:** To prevent unauthorized access to the camera's Web Configuration, you are strongly recommend to change the default administrator password. Type the administrator password twice to set and confirm the password.

- **General User**
  - **User Name/Password:** Enter the user's name you want to add to use the camera. Then, enter the password for the new user.

    After entering the User Name and Password, click **Add/Modify** to add the new user to the camera. To modify the user's information, select the one you want to modify from **UserList** and click **Add/Modify**.

  - **UserList:** Display the existing users of the camera. To delete a user, select the one you want to delete and click **Delete**.
- **Guest**
  - **User Name/Password:** Enter the user's name you want to add to use the camera. Then, enter the password for the new guest.

    After entering the User Name and Password, click **Add/Modify** to add the new user to the camera. To modify the user's information, select the one you want to modify from **UserList** and click **Add/Modify**.

  - **UserList:** Display the existing guests of the camera. To delete a user, select the one you want to delete and click **Delete**.

NOTE The "General User" can access the camera and control the Function buttons of the camera's Web Configuration; the "Guest' can only view the live view image from the Main screen of the Web Configuration while accessing the camera. Only the "Administrator" is allowed to configure the camera through the Web Configuration.

4.4 Network Settings

The Network menu contains the networking related settings for the camera, such as the IP Setting, DDNS Setting, IP Filter, and Wireless.

4.4.1 Network >> Network

- **IP Setting:** This item allows you to select the IP address mode and set up the related configuration. The default setting is **DHCP** mode enabled.
  - **DHCP:** Select this option when your network uses the DHCP server. When the camera starts up, it will be assigned an IP address from the DHCP server automatically.
  - **Static IP:** Select this option to assign the IP address for the camera directly. You can use IPFinder to obtain the related setting values.

IP	Enter the IP address of the camera. The default setting is 192.168.0.30.
Subnet Mask	Enter the Subnet Mask of the camera. The default setting is 255.255.255.0.
Default Gateway	Enter the Default Gateway of the camera. The default setting is 192.168.0.1.
Primary/ Secondary DNS	DNS (Domain Name System) translates domain names into IP addresses. Enter the Primary DNS and Secondary DNS that are provided by ISP.

  - **PPPoE:** Select this option when you use a direct connection via the ADSL modem. You should have a PPPoE account from your Internet service provider. Enter the **User Name** and **Password**. The camera will get an IP address from the ISP as starting up.

NOTE Once the camera gets an IP address from the ISP as starting up, it automatically sends a notification email to you. Therefore, when you select PPPoE as your connecting type, you have to set up the email or DDNS configuration in advance.

- **DDNS Setting:** With the Dynamic DNS feature, you can assign a fixed host and domain name to a dynamic Internet IP address. To set up the DDNS:
  1. Select the **Enable** option to enable this feature.

2. Select the **Provider** from the pull-down list.
3. Enter the required information in the **Host Name**, **User Name**, and **Password** boxes.

NOTE You have to sign up for DDNS service with the service provider before configuring this feature.

- **UPnP:** The camera supports UPnP (Universal Plug and Play), which is a set of computer network protocols that enable the device-to-device interoperability. In addition, it supports port auto mapping function so that you can access the camera if it is behind an NAT router or firewall. Select the **Enable** option to enable this feature.
- **Ports Number**
  - **HTTP Port:** The default HTTP port is **80**.

NOTE If the camera is behind an NAT router of firewall, the suggested to be used is from 1024 to 65535.

4.4.2 Network >> Network >> Advanced

- **Bonjour:** The devices with Bonjour will automatically broadcast their own services and listen for services being offered for the use of others. If your browser has Bonjour, you can find the camera on your local network without knowing its IP address.

  The Apple Safari is already with Bonjour. You can download the complete Bonjour for Internet Explorer browser from Apple's web site by visiting http://www.apple.com/bonjour/.
- **RTSP**
  - **RTSP Streaming:** Selection the **Authentication** as **Disable**, **Basic**, or **Digest** to configure the transmission of streaming data within the network.
  - **RTSP Port:** The default **RTSP Port** (Real Time Streaming Protocol) is **554**.

4.4.3 Network >> IP Filter

The IP Filter setting allows the administrator of the camera to limit the users within a certain range of IP addresses to access the camera. To disable this feature, select the **Disable** option; otherwise, select the **Accept** option to assign the range of IP addresses that are allowed to access the camera, or select the **Deny** option to assign the range of IP addresses that are blocked to access the camera.

- **Disable:** Select this option to disable the IP Filter function of the camera.
- **Accept**
  - **IPv4:** Assign a range of IP addresses that are allowed to access the camera by entering the **Start IP address** and **End IP address** options. When you are finished, click **Add** to save the range setting. You can repeat the action to assign multiple ranges for the camera.
  - **IPv6:** Enter the **IP Address** that is allowed to access the camera.
- **Deny**
  - **IPv4:** Assign a range of IP addresses that are blocked to access the camera by entering the **Start IP address** and **End IP address** options. When you are finished, click **Add** to save the range setting. You can repeat the action to assign multiple ranges for the camera.
  - **IPv6:** Enter the **IP Address** that is not allowed to access the camera.

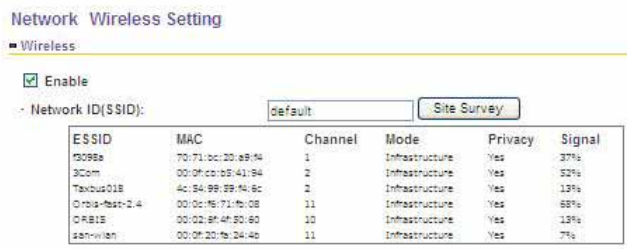
For example, when you enter *192.168.0.50/192.168.0.80* in **Start/End IP Address** of **Accept > IPv4**, the user whose IP address located within *192.168.0.50 ~ 192.168.0.80* will be allowed to access the camera. On the other hand, if you enter the IP range in **Start/End IP Address** of **Deny > IPv4**, the user whose IP address located within the range will not be allowed to access the camera.

4.4.4 Network >> Wireless Setting

The IPEyeAnywhere 241 / 341 supports WLAN while you use the wireless network. Select the **Enable** option to enable this feature.

- **Wireless**
  - **Network ID (SSID):** Keep the default setting of this option to connect the camera to any access point under the infrastructure network mode. To connect the camera to a specified access point, set a SSID for the camera to correspond with the access point's ESS-ID. To connect the camera to an Ad-Hoc wireless workgroup, set the same wireless channel and SSID to match with the computer's configuration.

Click **Site Survey** to display the available wireless networks, so that you can easily connect to one of the listed wireless networks.


Network Wireless Setting
Wireless
Enable
Network ID(SSID):
default
Site Survey
ESSID MAC Channel Mode Privacy Signal
f3098a 70:71:bc:20:a9:f4 1 Infrastructure Yes 37%
3Com 00:0f:cb:b5:41:84 2 Infrastructure Yes 52%
Taxbus018 4c:54:99:89:f4:6c 2 Infrastructure Yes 13%
Orbis-fast-2.4 00:0c:f6:71:fb:08 11 Infrastructure Yes 68%
ORBIS 00:02:6f:4f:50:60 10 Infrastructure Yes 13%
san-wlan 00:0f:20:fa:24:4b 11 Infrastructure Yes 7%

List of searching results

- **Wireless Mode:** Select the type of wireless communication for the camera: **Infrastructure** or **Ad-Hoc**.
- **Channel:** Select the appropriate channel from the list when you use an Ad-Hoc connection.
- **Authentication:** Select the authentication method to secure the camera from being used by unauthorized user: **Open**, **Shared-key**, **WPA-PSK**, and **WPA2-PSK**. The following table explains the four options:

Open	The default setting of Authentication mode, which communicates the key across the network.
Shared-key	Allow communication only with other devices with identical WEP settings.
WPA-PSK/ WPA2-PSK	WPA-PSK/WPA2-PSK is specially designed for the users who do not have access to network authentication servers. The user has to manually enter the starting password in their access point or gateway, as well as in each PC on the wireless network.

If you select **Open** or **Shared-key** as the Authentication mode, you need to complete the following settings:

- **Encryption:** Select the **WEP** option to enable the data encryption feature to secure the camera within the wireless network.
- **Format:** Once you enable the Encryption feature, you need to determine the encryption format by selecting **ASCII** or **HEX**. ASCII format causes each character you type to be interpreted as an eight-bit value. Hex format causes each pair of characters you type to be interpreted as an eight-bit value in hexadecimal (base 16) notation.
- **Key Length:** Select the WEP key length you use: **64 bits** or **128 bits**.
- **WEP Key 1/2/3/4:** Enter the WEP key(s) in the following boxes.

If you select **WPA-PSK** or **WPA2-PSK** as the Authentication mode, you need to complete the following settings:

- **Encryption:** Select **TKIP** or **AES**. TKIP (Temporal Key Integrity Protocol) changes the temporal key every 10,000 packets to insure much greater security than the standard WEP security. AES (Advanced Encryption Standard) is used to ensure the highest degree of security and authenticity for digital information.
- **Pre-Shared Key:** This is used to identify each other in the network. Enter the name in the box, and this name must match the Pre-shared key value in the remote device.

4.4.5 Network >> Wireless >> WPS Setting

WPS (Wi-Fi Protected Setup) sets a new standard of Wi-Fi security, providing a simplified secure network setup solution for the end users. Once the required settings have been completed, your wireless network can be protected by simply pressing the WPS button on the camera.

- **PROTECTED SETUP:** Press the **Reset to Unconfigured** button to reset the WPS configuration of the camera.
- **WPS**
  - **PIN Mode:** The PIN (Personal Information Number) mode builds the connection by entering the PIN Code directly. Once you enter the **PIN Code** of the camera on the router (or access point) that supports WPS, you can directly build a WPS connection between the camera and the device by simply pressing its WPS button.
  - **PBC Mode:** The PBC (Push Button Configuration) mode builds the connection by scanning the devices in the wireless network. Once you press the camera's WPS button, it starts to scan the WPS devices in the wireless network, and then you can build the WPS connection by clicking the **Connect** button.
- **Device Status:** Display the WPS configuration of the camera.

TIP The Power LED indicates the WPS connection status by:
- blinking 3 times when the connection is built successfully.
- repeating 3 times of short-short-long blink when the connection is failed.

4.5 Setting up Video & Audio

The Video & Audio menu contains four sub-menus that provide the video and audio settings for the camera.

4.5.1 Video & Audio >> Camera

- **Image Setting**
  - **Brightness:** Adjust the brightness level from 0 ~ 100.
  - **Saturation:** Adjust the colours level from 0 ~ 100.
  - **Sharpness:** Adjust the sharpness level from 0 ~ 100.

  TIP Click **Default** then **Apply** to restore the default settings of the three options above.

  - **Mirror:** Select **Vertical** to mirror the image vertically, or select **Horizontal** to mirror the image horizontally.

- **Light Frequency:** Select the proper frequency according to the camera's location to reduce the flicker: **50Hz**, **60Hz** or **Outdoor**.

TIP When the camera is installed indoors, the **Light Frequency** option can be set normally (**50Hz** or **60Hz**). However, the image of live video might be over exposure if the camera is focusing on the object outdoors. When this happens, you can set the option as **Outdoor** (even when the camera is installed indoors) to fix over exposure issue.

4.5.2 Video & Audio >> Video

- **H.264**
  - **Video Resolution:** Select the desired video resolution from the four formats: **SXGA**, **VGA**, **QVGA** and **QQVGA**. The higher setting (VGA) obtains better video quality while it uses more resource within your network.
  - **Video Quality:** Select the desired image quality from five levels: **Lowest**, **Low**, **Medium**, **High**, and **Highest**.
  - **Frame Rate:** Select a proper setting depending on your network status.
- **MPEG4**
  - **Video Resolution:** Select the desired video resolution from the three formats: **VGA**, **QVGA** and **QQVGA**. The higher setting (VGA) obtains better video quality while it uses more resource within your network.
  - **Video Quality:** Select the desired image quality from five levels: **Lowest**, **Low**, **Medium**, **High**, and **Highest**.
  - **Frame Rate:** Select a proper setting depending on your network status.
- **MJPEG**
  - **Video Resolution:** Select the desired video resolution from the four formats: **SXGA**, **VGA**, **QVGA** and **QQVGA**.

The higher setting (VGA) obtains better video quality while it uses more resource within your network.

- **Video Quality:** Select the desired image quality from five levels: **Lowest**, **Low**, **Medium**, **High**, and **Highest**.
- **Frame Rate:** Select a proper setting depending on your network status.

NOTE The camera supports H.264, MPEG4 and MJPEG compression. Please note that that MJPEG mode captures the images in JPEG format, which requires higher bandwidth to view smooth video. You can control the bandwidth of each connection well through the setting options above. For the bandwidth information, refer to the *Appendix, Bandwidth Reference Guide*.

- **3GPP:** The camera supports 3GPP specification. Select the **Disable** option to disable this feature. Otherwise, select **3GPP Without Audio** or **3GPP With Audio** to transfer the video clips without or with audio.

  If you use a mobile phone that supports 3GPP, you can also view the real-time streaming image captured by the camera on your phone (with the default player on the phone) by entering the RTSP link: rtsp://(IP address of the camera)/3gp.

NOTE Your mobile phone and the service provider must support 3GPP function. Please contact your service provider when you are failed to use this service.

4.5.3 Video & Audio >> Audio

- **Camera Microphone In:** Select the **Enable** option to enable the camera's audio function, so that you can receive the on-site sound and voice from the camera.
- **Camera Speaker Out:** Select the **Enable** option to enable the camera's external speaker function, so that the connected speaker can play the sound and voice through the camera.
  - **Volume:** Set the speaker's volume.

4.5.4 Video & Audio >> Overlay / Mask

This sub-menu is used to set the image overlay and mask feature of the camera.

- **Image Overlay:** This item allows you to set the image overlay.

  In the **Image File** option, click **Browse** to select the image file from your computer, and then click **Upload**. You can click **Preview** to check the image size and adjust the image position before clicking **Upload**. The preview image area is displayed with red dotted line. If you want to remove the preview image before uploading, click **Delete**.

  Since you click **Upload**, the preview image area is displayed with white dotted line. Click **Enable** and set the transparency setting by whether selecting the **Transparent** option or not.

  When done, click **Apply**. You can see the image overlay on the live view image when you click **Live View**.

NOTE The width and height of the input overlay graphic should be multiple of 4 at a maximum size of 43690 pixels, and in JPG or BMP (24-bit RGB) format.

- **Privacy Mask:** This item allows you to configure up to two mask areas.

Select the area 1 or 2 from the **Window** pull-down list, and then click **Enable**. You can change the size and position of the area by holding and dragging the mouse.

You can also change the colour of the mask area by clicking the **Colour** box and then selecting the colour you want.

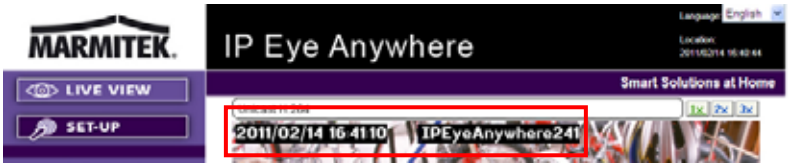
When done, click **Apply**. You can see the mask area(s) on the live view image when you click **Live View**.

4.5.5 Video & Audio >> Overlay / Mask >> Text Overlay

This page is used to set the text overlay feature of the camera, including the following three options: date & time, heading text, and background transparency setting.

- **Include Date & Time:** Select this option to display the date & time information on the live view image.
- **Include Text:** Select this option and enter your heading text in the box to display the text information on the live view image.
- **Enable Opaque:** Select this option to display the overlay text with a background colour.

For example, when you select the **Include Date & Time** and **Include Text** options and click **Apply**, you can see the related information on the live view image when you click **Live View**.



4.6 Event Server Configuration

The Event Server menu contains six sub-menus that allow you to upload images to FTP, send emails that include still images, store the images to a NAS system, send instant message, and upload the image/video to your Picasa/YouTube account.

When you complete the required settings for FTP, Email, or Network Storage, click **Test** to test the related configuration is correct or not. Once the camera connects to the server successfully, click **Apply**.

4.6.1 Event Server Setting >> FTP

- **FTP**
  - **Host Address:** Enter the IP address of the target FTP server.
  - **Port Number:** Enter the port number used for the FTP server.
  - **User Name:** Enter the user name to login into the FTP server.
  - **Password:** Enter the password to login into the FTP server.
  - **Directory Path:** Enter the destination folder for uploading the images. For example, /Test/.
  - **Passive Mode:** Select the **Enable** option to enable passive mode.
  - **FTP Upload with:** Select upload to FTP with one snapshot image or a series image in pre-event/post-event time when event triggered.

NOTE Due to the network environment, the camera may not upload number of images that you set.

4.6.2 Event Server Setting >> Email

- **Email**
  - **SMTP Server Address:** Enter the mail server address. For example, smtp.com.
  - **Sender Email Address:** Enter the email address of the user who will send the email. For example, mymail@mail.com.
  - **SMTP Port:** Assign the SMTP port in the text box. The default SMTP port is **25**. If the mail server requires an encrypted connection, you should check the SSL option.
  - **Authentication Mode:** Select **None** or **SMTP** according to the mail server configuration.

- **Sender User Name:** Enter the user name to login the mail server.
- **Sender Password:** Enter the password to login the mail server.
- **Receiver #1 Email Address:** Enter the first email address of the user who will receive the email.
- **Receiver #2 Email Address:** Enter the second email address of the user who will receive the email.
- **Send Email With:** Select the attachment type that is to be added to the email.

NOTE Due to the network environment, the camera may not upload number of images that you set.

4.6.3 Event Server Setting >> Network Storage

- **Network Storage**
  - **Samba Server Address:** Enter the IP address of the Network Storage server. For example, 192.168.1.12
  - **Share:** Assign the folder on the Network Storage server to share the files to users. For example, share
  - **Path:** Assign the path for uploading the files on the Network Storage server. For example, Test.
  - **User Name:** Enter the user name to login into the Network Storage server.
  - **Password:** Enter the password to login into the Network Storage server.
  - **Split By:** When the file is too large to upload smoothly, use this option to split it by selecting **File Size** or **Recording Time**.
  - **When Storage Full:** Select **Stop Recording** or **Recycle – Delete Oldest Folder** when the storage space on the Network Storage server is full.

- **Encode Format:** Select **MPEG4** or **H.264** as the encode format while recording.
- **File Format:** Select **MP4** or **AVI** as the file format while recording.

NOTE The recorded video files in Network Storage are enclosed by MP4/AVI format without audio.

4.6.4 Event Server Setting >> Instant Message

The camera supports the Jabber IM service, so that you can send an instant message once you have a Jabber account. For more information of Jabber, please visit the Jabber Website at: http://www.jabber.org/ .

- **Instant Message**
  - **Jabber ID:** Enter your user ID to login into the Jabber IM service.
  - **Jabber Password:** Enter the password to login into the Jabber IM service.
  - **Manually Specify Server Host/Port:** Select the Enable option to manually configure the Jabber server settings.
  - **Jabber Server Address:** Enter the Jabber server address manually.
  - **Jabber Port:** Assign the Jabber port manually in the text box.
  - **Encrypt Connection:** Select the **Enable** option to secure the connection.
  - **Encrypt Authentication:** Select the **Enable** option to secure the connection.
  - **Receiver:** Enter the receiver's information.
  - **Message:** Enter the message that is to be sent.

4.6.5 Event Server Setting >> Picasa Setting

The camera supports the Picasa upload service, so that you can send the camera's image to your Picasa account once you have a Picasa account.

- **Picasa Setting**
  - **User Name:** Enter your user name to login into the Picasa account.
  - **Password:** Enter the password to login into the Picasa account.
  - **Privacy:** Set the account as **Public** or **Private**.
  - **When Storage Full:** Select **Stop** or **Recycle – Delete Oldest Folder** when the storage space on the Picasa account is full.

4.6.6 Event Server Setting >> YouTube Setting

The camera supports the YouTube upload service, so that you can send the camera's video to your YouTube account once you have a YouTube account.

NOTE The USB Flash Disk must be mounted for YouTube upload.

- **YouTube Setting**
  - **User Name:** Enter your user name to login into the YouTube account.
  - **Password:** Enter the password to login into the YouTube account.
  - **Developer Key:** Enter the specify developer key if you have registered the Developer Key for YouTube.
  - **Source:** Enter the source code for YouTube.
  - **When Upload Fail:** Select the retry times (1~10) or interval time (in minute) to upload video again when upload is failed.
  - **Title:** Enter a title for the uploaded video.

- **Description:** Enter a description for the uploaded video.
- **Keyword:** Enter a keyword for the video so that the user can search the video easily.
- **Category:** Select a category for the uploaded video.
- **Privacy:** Set the account as **Public** or **Private**.

4.7 Motion Detect

The Motion Detect menu contains the command and option that allow you to enable and set up the motion detection feature of the camera. The camera provides three detecting areas.

To enable the detecting area, select **Window 1/2/3** from the pull-down list, and then select **Enable**. When the detecting area is enabled, you can use the mouse to move the detecting area and change the area coverage.

- **Name:** Assign a name to the detecting area.
- **Threshold:** Move the slide bar to adjust the level for detecting motion to record video.

NOTE Sliding the Threshold bar to the right will decrease the sensitivity of motion detection; sliding the Threshold bar to the left will increase the sensitivity of motion detection.

4.8 Event Configuration

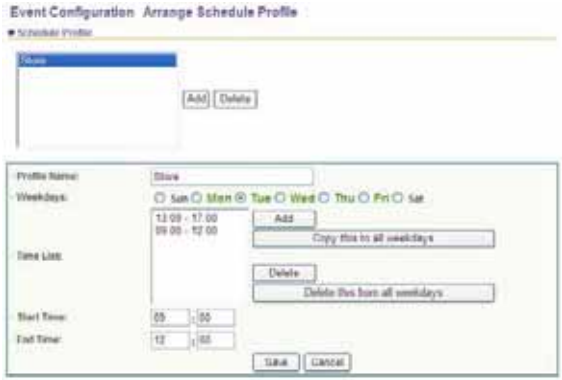
The Event Config menu contains five sub-menus that provide the commands to configure event profiles.

4.8.1 Event Configuration >> General Setting

- **General**
  - **Snapshot/Recording Subfolder:** You can assign a descriptive name for the subfolder to save the captured image/video files. Otherwise, leave this option blank to use the default setting.
  - **Storage Recording Time Per Event:** Limit the recording time while you are using the Network Storage solution.

4.8.2 Event Configuration >> Arrange Schedule Profile

- **Schedule Profile:** This sub-menu displays the scheduled profile(s). To customize the profile, click **Add** and then enter a descriptive name for the profile in the prompt dialog window. After entering the profile name, click **OK** and the profile is added to the Schedule Profiles list. To delete the profile, select the profile in the list and click **Delete**.



  - **Profile Name:** Display the profile name that you select in the Schedule Profiles list.
  - **Weekdays:** Select the weekday(s) that you want to separately assign in the schedule profile. The weekday that has been assigned will be displayed with green colour.
  - **Time List:** Display the time period that you have assigned within the selected weekday. To assign the same time period to every weekday, click **Copy this to all weekdays**; click **Delete this from all weekdays** to remove the selected time period from every weekday. Click Delete to remove the selected time period.
  - **Start/End Time:** Enter the start and end time and then click **Add** to assign a time period within in the selected weekday.

4.8.3 Event Configuration >> Motion Detect Trigger

- **Motion Detect Trigger:** Select the **Enable** option to enable the trigger function of the camera, so that you can send captured images within the detecting area to the FTP server, email receiver, or the Network Storage server, etc. You have to configure corresponding settings, such as FTP server and email server, to enable this feature. Please note that you have to configure the related settings before enabling these features.
  - **Schedule Profile:** Select a schedule profile from the pull-down list.
  - **Action:** Select the destination that the captured images will be sent to: **Record to USB (Upload to YouTube)**, **Record to Network Storage**, **Send Email**, **FTP Upload**, **Instant Message**, or **Upload Image to Picasa**.

4.8.4 Event Configuration >> Schedule Trigger

You can separately configure the schedule for trigger function of the camera by **Email**, **FTP**, or **Network Storage**. Select the **Enable** option on each item, and then select a **Schedule Profile** from the pull-down list and set the **Interval** time.

NOTE If the setting value of the **Storage Recording Time Per Event** option in General Setting is longer than the **Interval** time in Network Storage Schedule, the recorded file will be a continuous video clip.

For example, if you set the **Storage Recording Time Per Event** as 10 seconds and the **Interval** as 5 seconds, recorded file becomes a non-stop video clip because the camera will record a 10-second video clip every 5 seconds.

4.9 Tools

The Tools menu provides the commands that allow you to restart or reset the camera. You can also backup and restore your configuration, and upgrade the firmware for the camera.

- **Factory Reset:** Click **Reset** to restore all factory default settings for the IP EyeAnywhere.
- **System Reboot:** Click **Reboot** to restart the camera just like turning the device off and on. The camera configuration will be retained after rebooting.
- **Configuration:** You can save your camera configuration as a backup file on your computer. Whenever you want to resume the original settings, you can restore them by retrieving the backup file.

- **Backup:** Click **Get the backup file** to save the current configuration of the camera.
- **Restore:** Click **Browse** to locate the backup file and then click **Restore**.

- **Update Firmware:** You can upgrade the firmware for your camera once you obtained a latest version of firmware.
  - **Current Firmware Version:** This item displays the current firmware version.
  - **Select the firmware:** Click **Browse** to locate the backup file and then click **Update**.

NOTE Make sure to keep the camera connected to the power source during the process of upgrading firmware. Otherwise, the camera might be damaged because of failure of upgrading firmware.

When this happens, the system will enable the Rescue mode (as shown below) after the camera reboots, so that you can upgrade the firmware again.

4.10 USB

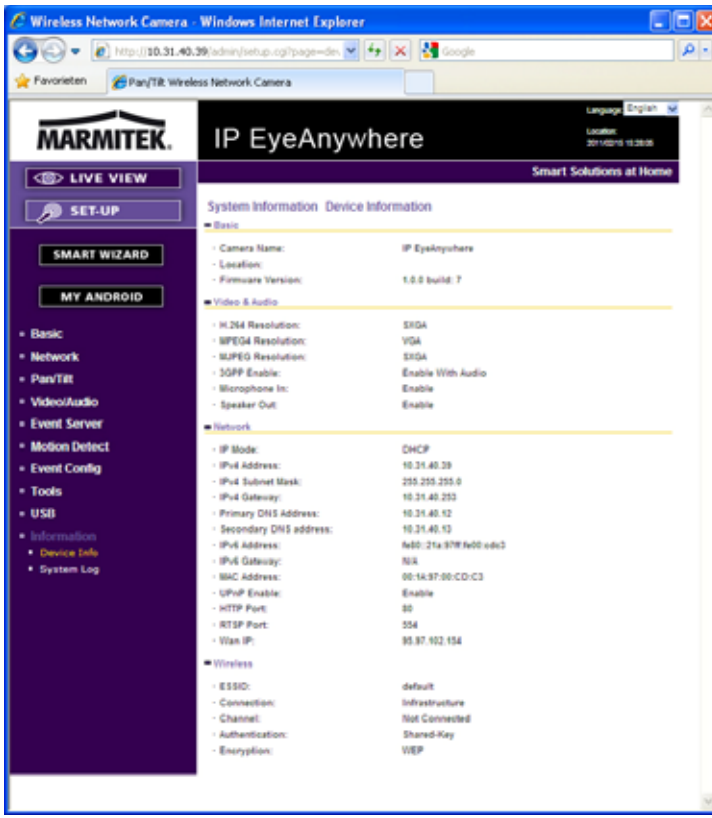
The USB menu provides the information and controls of the connected USB device.

- **USB Dismount:** To safely remove the connected USB device, you can press the Unmount button for four seconds on the camera or click **Dismount** from this item.
- **USB Information:** Display the **Total space** and **Free space** of the USB device.
- **USB Setting**
  - **Split By:** When the file is too large to transfer smoothly, use this option to split it by selecting **File Size** or **Recording Time**.

- **When Storage Full:** Select **Stop Recording** or **Recycle – Delete Oldest Folder** when the storage space on the USB device is full.
- **Encode Format:** Set the encode format of the captured image as **MJPEG** or **H.264**.
- **File Format:** Set the file format of the recorded video as **MP4** or **AVI**.
- **Upload the Recorded file to YouTube:** Select the option to simultaneously upload the recorded video file to the YouTube account that you have assigned.
-

4.11 Information

The Information menu displays the current configuration and events log of the camera.



- **Device Info:** Display the Basic, Video & Audio, and Network settings of the camera.
- **System Log:** The Logs table displays the events log recorded by the system.

Appendix

A.1 Specification

- **Image Sensor**

Sensor	1/4” Colour Megapixel CMOS Sensor
Resolution	1280 x 1024
Min. Illumination	0,5 Lux
IR blocking filter	IPEA 341
True Colour	IPEA 341

- **System Hardware**

Processor	ARM9 base
RAM	64MB SDRAM
ROM	8MB NOR Flash
Power	DC 12V
Power Consumption	10W max.

- **Lens Assembly**

Lens Type	Board Lens
Lens Specification	F2.8, 4.0mm
View Angle	60 degree
Night vision	940nm IR LED (Switch by light sensor, manually and schedule control, IPEA 241)

- **Video**

Compression	H.264/MPEG4/MJPEG
Video resolution	H.264 & MJPEG: SXGA (1280 x 1024) @ 15fps / VGA (640 x 480) @ 30fps / QVGA (320 x 240) @ 30fps / QQVGA (160 x 120) @ 30fps; MPEG4: VGA (640 x 480) @ 30fps / QVGA (320 x 240) @ 30fps / QQVGA (160 x 120) @ 30fps

- **Communication**

LAN	10/100Mbps Fast Ethernet with Auto-MDIX
WLAN	(for wireless model) IEEE 802.11b/g/n
Protocol support	TCP/IP,IPV6, UDP, ICMP,DHCP client, NTP, DNS, DDNS, SMTPs, FTP, HTTP, Samba, UPnP, RTP, RTCP, RTSP

- **Audio**

Input	Built-in microphone
Output	Headphone output jack (Mono)
Codec	PCM/AMR (AMR is for 3GPP only)

- **User Interface**

LAN	One RJ-45 port
Antenna	One external antenna
USB Port	USB 2.0 port, with one unmount button; Power distribution: 500mA Max.
USB Dismount	One USB Dismount button
Reset	One Reset button
WPS	One WPS button
LEDs	Power LED (amber); Link LED (green)

- **Software**

OS Support	Windows XP/Vista, and Windows 7/8
Browser	Internet Explorer 6.0 or above; Apple Safari 2 or above; Mozilla Firefox 2.00 or above
Software	UltraView Pro for playback/recording/ configuration features

- **Operating Environment**

Temperature	Operation: 0°C ~ 45°C; Storage: -15°C ~ 60°C
Humidity	Operation: 20% ~ 85% non-condensing; Storage: 0% ~ 90% non-condensing

- **EMI** LVD, EuP Power report (ERP), FCC/CE class B

A.3 Glossary of Terms

NUMBERS

10BASE-T 10BASE-T is Ethernet over UTP Category III, IV, or V unshielded twisted-pair media.

100BASE-TX The two-pair twisted-media implementation of 100BASE-T is called 100BASE-TX.

A

ADPCM Adaptive Differential Pulse Code Modulation, a new technology improved from PCM, which encodes analog sounds to digital form.

AMR AMR (Adaptive Multi-Rate) is an audio data compression scheme optimized for speech coding, which is adopted as the standard speech codec by 3GPP.

Applet Applets are small Java programs that can be embedded in an HTML page. The rule at the moment is that an applet can only make an Internet connection to the computer form that the applet was sent.

ASCII American Standard Code For Information Interchange, it is the standard method for encoding characters as 8-bit sequences of binary numbers, allowing a maximum of 256 characters.

ARP Address Resolution Protocol. ARP is a protocol that resides at the TCP/IP Internet layer that delivers data on the same network by translating an IP address to a physical address.

AVI Audio Video Interleave, it is a Windows platform audio and video file type, a common format for small movies and videos.

B

BOOTP Bootstrap Protocol is an Internet protocol that can automatically configure a network device in a diskless workstation to give its own IP address.

C

Communication Communication has four components: sender, receiver, message, and medium. In networks, devices and application tasks and processes communicate messages to each other over media. They represent the sender and receivers. The data they send is the message. The cabling or transmission method they use is the medium.

Connection In networking, two devices establish a connection to communicate with each other.

D

DHCP Developed by Microsoft, DHCP (Dynamic Host Configuration Protocol) is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. It also supports a mix of static and dynamic IP addresses. This simplifies the task for network administrators because the software keeps track of IP addresses rather than requiring an administrator to manage the task. A new computer can be added to a network without the hassle of manually assigning it a unique IP address. DHCP allows the specification for the service provided by a router, gateway, or other network device that automatically assigns an IP address to any device that requests one.

DNS Domain Name System is an Internet service that translates domain names into IP addresses. Since domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses every time you use a domain name the DNS will translate the name into the corresponding IP address. For example, the domain name *www.network_camera.com* might translate to *192.167.222.8*.

E

Enterprise An enterprise network consists of collections of

network networks connected to each other over a geographically dispersed area. The enterprise network serves the needs of a widely distributed company and operates the company's mission-critical applications.

Ethernet The most popular LAN communication technology. There are a variety of types of Ethernet, including 10Mbps (traditional Ethernet), 100Mbps (Fast Ethernet), and 1,000Mbps (Gigabit Ethernet). Most Ethernet networks use Category 5 cabling to carry information, in the form of electrical signals, between devices. Ethernet is an implementation of CSMA/CD that operates in a bus or star topology.

F

Fast Ethernet Fast Ethernet, also called 100BASE-T, operates at 10 or 100Mbps per second over UTP, STP, or fiber-optic media.

Firewall Firewall is considered the first line of defense in protecting private information. For better security, data can be encrypted. A system designed to prevent unauthorized access to or from a private network. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially Intranets all messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

G

Gateway A gateway links computers that use different data formats together.

Group Groups consist of several user machines that have similar characteristics such as being in the same department.

H

HEX Short for hexadecimal refers to the base-16 number system, which consists of 16 unique symbols: the

numbers 0 to 9 and the letters A to F. For example, the decimal number 15 is represented as F in the hexadecimal numbering system. The hexadecimal system is useful because it can represent every byte (8 bits) as two consecutive hexadecimal digits. It is easier for humans to read hexadecimal numbers than binary numbers.

I

Intranet This is a private network, inside an organization or company that uses the same software you will find on the public Internet. The only difference is that an Intranet is used for internal usage only.

Internet The Internet is a globally linked system of computers that are logically connected based on the Internet Protocol (IP). The Internet provides different ways to access private and public information worldwide.

Internet address To participate in Internet communications and on Internet Protocol-based networks, a node must have an Internet address that identifies it to the other nodes. All Internet addresses are IP addresses

IP Internet Protocol is the standard that describes the layout of the basic unit of information on the Internet (the *packet*) and also details the numerical addressing format used to route the information. Your Internet service provider controls the IP address of any device it connects to the Internet. The IP addresses in your network must conform to IP addressing rules. In smaller LANs, most people will allow the DHCP function of a router or gateway to assign the IP addresses on internal networks.

IP address IP address is a 32-binary digit number that identifies each sender or receiver of information that is sent in packets across the Internet. For example 80.80.80.69 is an IP address. When you “call” that number, using any connection methods, you get connected to the computer that “owns” that IP address.

ISP ISP (Internet Service Provider) is a company that maintains a network that is linked to the Internet by

way of a dedicated communication line. An ISP offers the use of its dedicated communication lines to companies or individuals who can't afford the high monthly cost for a direct connection.

J

JAVA Java is a programming language that is specially designed for writing programs that can be safely downloaded to your computer through the Internet without the fear of viruses. It is an object-oriented multi-thread programming best for creating applets and applications for the Internet, Intranet and other complex, distributed network.

L

LAN Local Area Network a computer network that spans a relatively small area sharing common resources. Most LANs are confined to a single building or group of buildings.

M

MJPEG MJPEG (Motion JPEG) composes a moving image by storing each frame of a moving picture sequence in JPEG compression, and then decompressing and displaying each frame at rapid speed to show the moving picture.

MPEG4 MPEG4 is designed to enable transmission and reception of high-quality audio and video over the Internet and next-generation mobile telephones.

N

NAT Network Address Translator generally applied by a router that makes many different IP addresses on an internal network appear to the Internet as a single address. For routing messages properly within your network, each device requires a unique IP address. But the addresses may not be valid outside your network. NAT solves the problem. When devices within

	your network request information from the Internet, the requests are forwarded to the Internet under the router's IP address. NAT distributes the responses to the proper IP addresses within your network.
Network	A network consists of a collection of two or more devices, people, or components that communicate with each other over physical or virtual media. The most common types of network are: **LAN** – (local area network): Computers are in close distance to one another. They are usually in the same office space, room, or building. **WAN** – (wide area network): The computers are in different geographic locations and are connected by telephone lines or radio waves.
NWay Protocol	A network protocol that can automatically negotiate the highest possible transmission speed between two devices.

P

PCM	PCM (Pulse Code Modulation) is a technique for converting analog audio signals into digital form for transmission.
PING	Packet Internet Groper, a utility used to determine whether a specific IP address is accessible. It functions by sending a packet to the specified address and waits for a reply. It is primarily used to troubleshoot Internet connections.
PPPoE	Point-to-Point Protocol over Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as DSL or cable modem. All the users over the Ethernet share a common connection.
Protocol	Communication on the network is governed by sets of rules called protocols. Protocols provide the guidelines devices use to communicate with each other, and thus they have different functions. Some protocols are responsible for formatting and presenting and presenting data that will be transferred from file server

memory to the file server's net work adapter Others are responsible for filtering information between networks and forwarding data to its destination. Still other protocols dictate how data is transferred across the medium, and how servers respond to workstation requests and vice versa. Common network protocols responsible for the presentation and formatting of data for a network operating system are the Internetwork Packet Exchange (IPX) protocol or the Internet Protocol (IP). Protocols that dictate the format of data for transferors the medium include token-passing and Carrier Sense Multiple Access with Collision Detection (CSMA/CD), implemented as token-ring, ARCNET, FDDI, or Ethernet. The Router Information Protocol (RIP),a part of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite, forwards packets from one network to another using the same network protocol.

R

RJ-45 RJ-45 connector is used for Ethernet cable connections.

Router A router is the network software or hardware entity charged with routing packets between networks.

RTP RTP (Real-time Transport Protocol) is a data transfer protocol defined to deliver **live media** to the clients at the same time, which defines the transmission of video and audio files in real time for Internet applications.

RTSP RTSP (Real-time Streaming Protocol) is the standard used to transmit **stored media** to the client(s) at the same time, which provides client controls for random access to the content stream.

S

Server It is a simple computer that provides resources, such as files or other information.

SIP SIP (Session Initiated Protocol) is a standard protocol that delivers the real-time communication for Voice over IP (VoIP), which establishes sessions for features such as audio and video conferencing.

SMTP The Simple Mail Transfer Protocol is used for Internet mail.

SNMP Simple Network Management Protocol. SNMP was designed to provide a common foundation for managing network devices.

Station In LANs, a station consists of a device that can communicate data on the network. In FDDI, a station includes both physical nodes and addressable logical devices. Workstations, single-attach stations, dual-attach stations, and concentrators are FDDI stations.

Subnet mask In TCP/IP, the bits used to create the subnet are called the subnet mask.

T

(TCP/IP) Transmission Control Protocol/Internet Protocol is a widely used transport protocol that connects diverse computers of various transmission methods. It was developed y the Department of Defense to connect different computer types and led to the development of the Internet.

Transceiver A transceiver joins two network segments together. Transceivers can also be used to join a segment that uses one medium to a segment that uses a different medium. On a 10BASE-5 network, the transceiver connects the network adapter or other network device to the medium. Transceivers also can be used on 10BASE-2 or 10BASE-T networks to attach devices with AUI ports.

U

UDP The User Datagram Protocol is a connectionless protocol that resides above IP in the TCP/IP suite

User Name The USERNAME is the unique name assigned to each person who has access to the LAN.

Utility It is a program that performs a specific task.

UTP Unshielded twisted-pair. UTP is a form of cable used by all access methods. It consists of several pairs of

wires enclosed in an unshielded sheath.

W

WAN Wide-Area Network. A wide-area network consists of groups of interconnected computers that are separated by a wide distance and communicate with each other via common carrier telecommunication techniques.

WEP WEP is widely used as the basic security protocol in Wi-Fi networks, which secures data transmissions using 64-bit or 128-bit encryption.

Windows Windows is a graphical user interface for workstations that use DOS.

WPA WPA (Wi-Fi Protected Access) is used to improve the security of Wi-Fi networks, replacing the current WEP standard. It uses its own encryption, Temporal Key Integrity Protocol (TKIP), to secure data during transmission.

WPA2 Wi-Fi Protected Access 2, the latest security specification that provides greater data protection and network access control for Wi-Fi networks. WPA2 uses the government-grade AES encryption algorithm and IEEE 802.1X-based authentication, which are required to secure large corporate networks.

MARMITEK®

www.marmitek.com